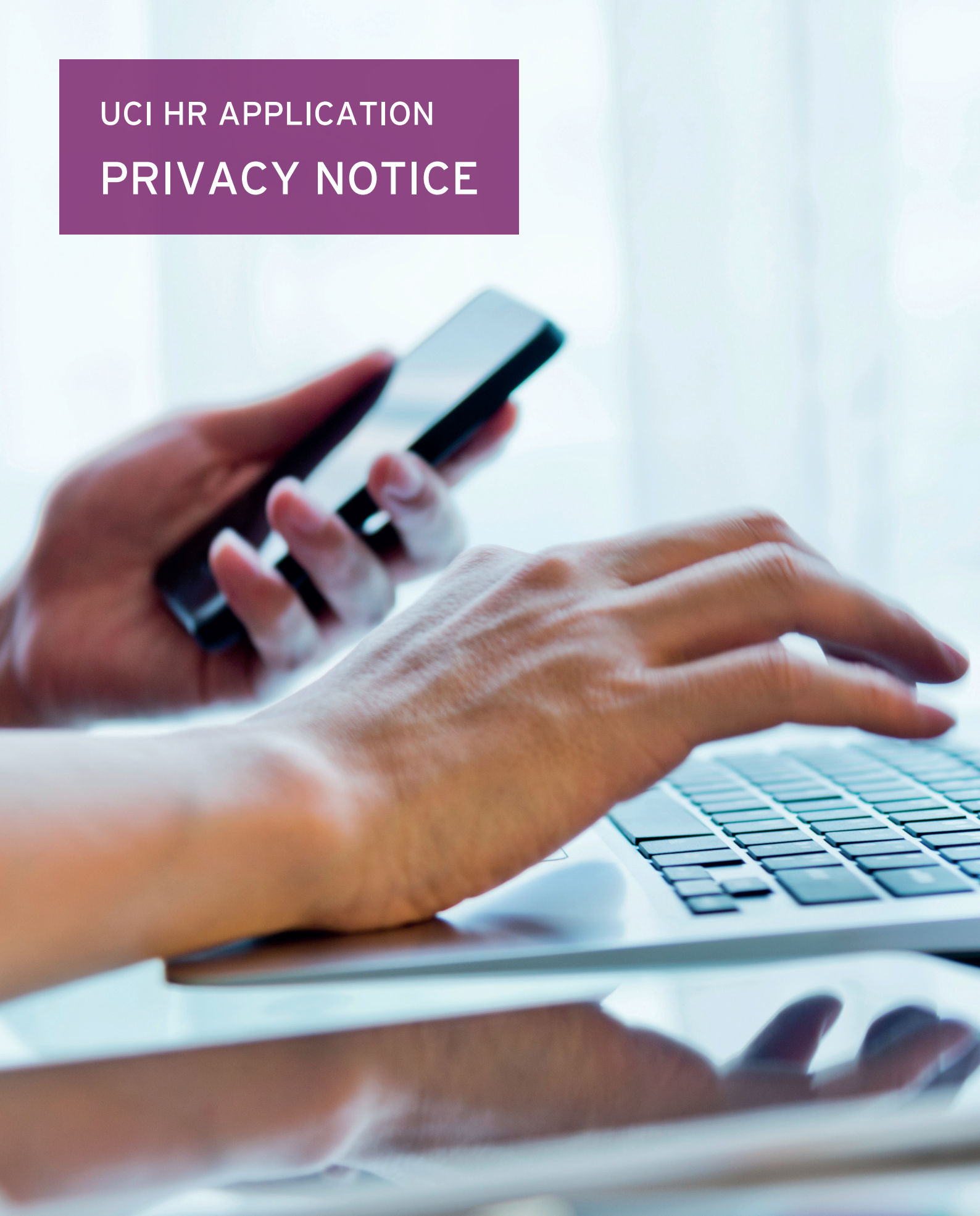


UCI HR APPLICATION PRIVACY NOTICE



UCI HR Application Privacy Notice

We take the privacy and security of your personal data very seriously and at all times we will comply with the prevailing laws and regulations governing confidentiality, data protection and security of information.

This privacy policy explains how we use your personal data in the course of your application for a role with Computershare. It also explains your rights over your personal information, and how you can exercise them.

If you have any questions about this privacy policy or how we use your personal data, please contact our Data Protection Officer by writing to: The Pavilions, Bridgwater Road, Bristol, BS13 8AE or you can email us.

Who we are

Depending on the UK, Channel Islands, Ireland or Spain (UCI) Computershare business you are applying to, if successful in your application you will be employed by one of the following companies:

- Computershare Services Limited
- Computershare Investor Services PLC
- Homeloan Management Limited
- Computershare Mortgage Services Limited
- Credit Advisory Services Limited
- Topaz Finance Limited
- Computershare Technology Services (UK) Limited
- Computershare Investor Services (Ireland) Limited
- Computershare Investor Services (Jersey) Limited
- Computershare Investor Services (Guernsey) Limited
- Computershare Global Technology Services (UK) Limited
- Computershare Governance Services
- Computershare Limited

Within this document we will refer to these companies as “we”, “us” or “our”.

Across the UCI region, we process your personal data using common processes and this privacy notice covers all of the above companies.

What Personal Data do we use?

To process your application we will use the following information about you.

- Personal details such as your full name (and any maiden or previous name), current and previous addresses, nationality, date of birth, marital status and dependents, telephone numbers, e-mail addresses and passport, driving licence, National Identifier, ethnic origin and disability details;
- Details of your emergency contact(s)
- Details of your employment circumstances such as your current role, salary, pension, benefits information;
- Recruitment information (including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process);
- Bank account details (Account Number, Sort Code and Bank Name);
- Information from Fraud Prevention Agencies;
- Information from Law Enforcement and Crime Reference Agencies; and
- Information from Credit Reference Agencies.

UCI HR Application Privacy Notice

Where do we obtain your data from?

Much of the personal data we collect will be provided directly by you when you first apply for a role with us or when you communicate with us during the course of your application.

We will also obtain data from the following third parties in the course of your application:

- Credit Reference Agencies;
- Fraud and crime prevention agencies;
- Individuals or organisations you authorise us to seek references from; and
- Public bodies (such as law enforcement agencies, regulatory authorities or tax agencies).

In addition, we will also collect information about you which can be obtained via open data sources and public records (e.g. the electoral register and information openly available via the internet), although we will only do this where it relates to your application for employment and our assessment of this application.

How do we use your data?

We use your personal data to:

- validate your identity;
- identify you when you contact us;
- perform credit checks;
- perform criminal records checks;
- carry out background and reference checks;
- assess your suitability for a role (including checking you are legally entitled to work in the country you have applied for a job in);
- prevent fraud and assess other relevant conduct;
- respond to enquiries which you make;
- keep records relating to our hiring processes;
- monitor and report compliance with applicable legislation and regulation; and
- manage our business in an efficient and proper manner, including the management of our financial position, our resources, the risks to which we are exposed and the way in which we arrange our internal operations.

If you fail to provide information when requested, which is necessary for us to consider your application (such as evidence of qualifications or work history), we will not be able to process your application successfully. For example, if we require a credit check or references for this role and you fail to provide us with relevant details, we will not be able to take your application further.

Information about criminal convictions

We envisage that we will process information about criminal convictions.

We will collect information about your criminal convictions history where we would like to offer you the role (conditional on checks and any other conditions, such as references, being satisfactory). We are entitled to carry out a criminal records check in order to satisfy ourselves that there is nothing in your criminal convictions history which makes you unsuitable for the role. In particular, working within Computershare you would have access to confidential personal and financial information and so we would seek a disclosure of your criminal records history.

UCI HR Application Privacy Notice

Automated Decision Making

Within the recruitment process, you may be subject to decisions that will have a significant impact on you based solely on automated decision-making. Specifically, the online recruitment process will automatically decline applications where:

- You have stated that you do not have the right to work in the country you are applying to work in; or
- You have stated that you do not have the required qualifications or experience for the role applied for.

This automated decision making is applied as having the right to work in the country and having the qualifications/experience required for the role are required for us to enter into a contract of employment with you.

What are our legal reasons for processing your data?

Where we process your personal data, we need to have a valid legal basis for doing so. In relation to your application the legal basis for processing your personal data are:

- because the processing is necessary for us to take steps, at your request, to enter into an employment contract with you;
- because it is necessary to comply with a legal obligation including financial crime and employment legislation;
- because you have consented to a specific use of your data. This would apply if you have consented to us using your special category data for equal opportunities monitoring purposes; or
- because it is necessary for the purposes of our legitimate interests. This applies to circumstances where processing is not necessary for entering into a contract with you such as analysis and reporting to support internal management and governance of our business. It also applies to circumstances where we disclose your data to Fraud Prevention Agencies, including CIFAS in the UK, for the prevention of fraud and other relevant conduct.

Who do we share your personal data with?

To enable us to process your application and enter into an employment contract with you we will share your personal data with:

- other Computershare group companies;
- non-Computershare companies to whom we outsource the delivery of some of our services;
- non-Computershare companies who help us with administrative services, including printing, mailing and IT services;
- non-Computershare companies who help us with pre-employment screening and background checking;
- credit reference agencies;
- secure information storage and destruction providers;
- our legal or other professional advisors, including our auditors;
- public bodies (such as law enforcement agencies, regulatory authorities or tax agencies);
- fraud and crime prevention agencies (including CIFAS in the UK); and
- courts, to comply with legal requirements, and for the administration of justice.

Transferring your personal data outside the European Economic Area

In the course of your application your personal data will be sent outside of the European Economic Area.

While some countries have adequate protections for personal data under applicable laws, in other countries steps will be taken to ensure appropriate safeguards apply to it. These include imposing contractual obligations to implement safeguards that protect your data and ensure you can exercise your rights.

UCI HR Application Privacy Notice

How long will we keep your personal data?

Where personal data is collected to progress a job application that does not complete, this personal data will be retained for a period of 6 months unless you provide consent for your data to be held for longer.

Your Rights

Accessing your information

- You may ask for a copy of the personal information we hold about you by writing to us.

Correcting your information

- We try to ensure all of the personal data we hold is accurate. If you find any inaccuracies or if your details change, please notify us promptly and we will correct them.

Erasing or restricting use of your information

- You may ask us to erase or restrict use of your personal information. If you do, we will comply with your request unless there is a legal reason for us not to.

Withdrawing consent

- Where the legal basis for us processing your personal information is that you have given your consent to that processing, you may withdraw your consent at any time. If you do so we will stop processing your personal data promptly.

Objecting to processing

- object to our processing of your personal data where it is based exclusively on our legitimate interests.

To exercise one or more of these rights please write to:

hrrservices@computershare.co.uk

HR Services

The Pavilions

Bridgewater Road

Bristol

BS13 8AE

Please note that we may ask you to provide a form of identification verification before we can give effect to any such request made by you.

Complaints

If you have any complaints about the way we use your personal information please contact our Data Protection Officer who will try to resolve the issue.

You have the right to complain to the data protection supervisory authority in your country.

UK - Information Commissioner's Office - ico.org.uk

Jersey - Office of the Information Commissioner - oicjersey.org

Guernsey - Office of the Data Protection Commissioner - dataci.gg

Ireland - Office of the Data Protection Commissioner - www.dataprotection.ie

Spain - Agencia Espanola De Proteccion De Datos - www.agpd.es

UCI HR Application Privacy Notice

Appendix 1 - Credit Reference Agencies

The Credit Reference Agencies which we may use are:

- CallCredit Ltd;
- Equifax Ltd;
- Experian Ltd; and
- Irish Credit Bureau D.A.C.

For further information regarding how credit reference agencies use your data see the Credit Reference Agencies Information Notice, available at:

www.equifax.co.uk/crain;

www.callcredit.co.uk/crain;

www.experian.co.uk/crain; and

www.icb.ie/pdf/Fair%20Processing%20Notice.pdf.

Appendix 2 - Fraud Prevention Agencies

We and other organisations may access and use your information to prevent fraud.

In the UK we will check your details against the Cifas databases established for the purpose of allowing organisations to record and share data on their fraud cases, other unlawful or dishonest conduct, malpractice, and other seriously improper conduct ("Relevant Conduct") carried out by their staff and potential staff. "Staff" means an individual engaged as an employee, director, trainee, homeworker, consultant, contractor, temporary or agency worker, or self-employed individual, whether full or part time or for a fixed-term

The personal data you have provided, we have collected from you, or we have received from third parties will be used to prevent fraud and other relevant conduct and to verify your identity.

Details of the personal information that will be processed include: name, address, date of birth, any maiden or previous name, contact details, document references, National Insurance Number, and nationality. Where relevant, other data including employment details will also be processed.

We and Cifas may also enable law enforcement agencies to access and use your personal data to detect, investigate, and prevent crime.

We process your personal data on the basis that we have a legitimate interest in preventing fraud and other Relevant Conduct, and to verify identity, in order to protect our business and customers and to comply with laws that apply to us. This processing of your personal data is also a requirement of your engagement with us.

Cifas will hold your personal data for up to six years if you are considered to pose a fraud or Relevant Conduct risk.

Should our investigations identify fraud or any other Relevant Conduct by you when applying for or during the course of your engagement with us, your new engagement may be refused or your existing engagement may be terminated or other disciplinary action taken (subject to your rights under your existing contract and under employment law generally).

A record of any fraudulent or other Relevant Conduct by you will be retained by Cifas and may result in others refusing to employ you. If you have any questions about this, please contact us using the details provided.

Cifas may allow the transfer of your personal data outside of the UK. This may be to a country where the UK Government has decided that your data will be protected to UK standards, but if the transfer is to another type of country, then Cifas will ensure your data continues to be protected by ensuring appropriate safeguards are in place. Your personal data is protected by legal rights, which include your rights to object to our processing of your personal data, request that your personal data is erased or corrected, and request access to your personal data.

For more information or to exercise your data protection rights please, please contact us using the contact details provided.

You also have a right to complain to the Information Commissioner's Office which regulates the processing of personal data.

